We Claim:

1. A method for selecting at least one encryption key used to encrypt a data message having at least one message data block prior to transmitting said encrypted message blocks over a network, said method comprising the steps of:

a. extracting a data value from a message data block;

b. selecting an encryption key from among a plurality of encryption key;

c. encrypting a subsequent message data block using said selected encryption key; and

d. transmitting said encrypted data block over said network

2. The method as recited in Claim 1 wherein

steps a-d are iteratively repeated for each message data block.

3. The method as recited in Claim 1 further comprising the steps of

a. receiving said encrypted data blocks;

b. decrypting said received data block using an key based a prior data block;

c. extracting a data value from a message data block; and

d. selecting an encryption key from among a plurality of retained encryption keys.

4. The method as recited in claim 1 wherein said extracted a data value is determined using a known number of bits.

5. The method as recited in claim 4 wherein said known number of bits are distributed among at least one byte of said data block

6. The method as recited in claim 4 wherein said known number of bits are located in a first byte of each of said message blocks.

7. The method as recited in claim 4 wherein said known number of bits are located in a last byte of each of said message blocks.

8. The method as recited in claim 1 wherein said data block corresponds to at least one unencrypted data block.

9. The method as recited in claim 1 wherein said data block corresponds to a synchronizing indicator.

10. The method as recited in claim 1 wherein said step of extracting further comprises limiting said extracted data value to a known range.

11. The method as recited in claim 10 wherein said know range is determined using modulo-arithmetic.

12. The method as recited in claim 10 wherein said known range is substantially comparable to a number of said stored encryption keys.

13. A system for selecting at least one encryption key used to encrypt a data message having at least one message data block prior to transmitting said encrypted message blocks over a network, said system comprising:

a communication apparatus operative to:

extract a data value from each of said at least one message data blocks;

select an encryption key from among a plurality of encryption key stored in a memory;

encrypt at least one subsequent message data block using said selected encryption key; and

transmit said encrypted message data block over said network.

14. The system as recited in claim 13 further comprising

a second communication apparatus operative to:

receive said at least one transmitted encrypted data block;

extract a data value from each of said previously transmitted data blocks;

select an decryption key from among a plurality of decryption keys stored said memory based on said extracted data value; and

decrypt said at least one received message using said selected key.

15. The system as recited in claim 13 wherein said extracted a data value is determined using a known number of bits.

16. The system as recited in claim 15 wherein said known number of bits are distributed among at least one byte of said data block

17. The system as recited in claim 15 wherein said known number of bits are located in a first byte of each of said message blocks.

18. The system as recited in claim 15 wherein said known number of bits are located in a last byte of each of said message blocks.

19. The system as recited in claim 13 wherein said data block corresponds to at least one unencrypted data block.

20. The system as recited in claim 13 wherein said data block corresponds to a synchronization indicator.

21. The system as recited in claim 13 wherein said apparatus is further operative to select said encryption key based on said extracted data value.

22. The system as recited in claim 21 wherein said apparatus is further operative to limit said extracted data value to a known range.

23. The system as recited in claim 22 wherein said known range is substantially comparable to a number of said plurality of encryption keys.

24. A device to determine at least one encryption key from a plurality of encryption keys, stored in a memory, said encryption key used to encrypt a message composed of data message blocks, said device comprised of:

a processor, in communication with said memory, operative to:

extract a known number data bits from a data message block;

select an encryption key from said stored encryption keys based on content of said known number of data bits; and

encrypt a subsequent message data block using said selected encryption key; and

a transmitting device, in communication with said processor to transmit said encrypted data block.

25. The device as recited in claim 24 further comprising

a receiving device to receive a transmitted data message block;

a processor, in communication with said receiving device, operative to:

extract said known number of data bits from a previously received message data block;

select a decryption key from a plurality of decryption keys stored in said memory based on content of a known data item; and

decrypt said received data block using said selected decryption key.

26. The device as recited in claim 24 wherein said known number of bits are distributed among at least one byte of said data block

27. The device as recited in claim 24 wherein said known number of bits are located in a first byte of each of said message data blocks.

28. The device as recited in claim 24 wherein said known number of bits are located in a last byte of each of said message data blocks.

29. The device as recited in claim 24 wherein said data block corresponds to at least one unencrypted data block.

30. The device as recited in claim 29 wherein said data block corresponds to a synchronization indicator.

31. The device as recited in claim 24 wherein said processor is further operative to limit said extracted data value to a known range.

32. The device as recited in claim 31 wherein said known range is substantially comparable to a number of said plurality of encryption keys.